

Claims

1. Method of securing patient data in the case of an exchange of information through a data network with the aid of computers, wherein the patient's name and address is entered in a first form displayed on a screen of a computer,
the patient is assigned an identification number, which is displayed on the screen,
the identification number and a question are entered in a second form displayed on a screen,
the answer to the question is assigned to the identification number and displayed on a screen when the identification number is specified.
2. Method of Claim 1, wherein the patient's name and address on the one hand and the question and answer on the other hand are processed and stored on separate Web servers and/or separate database servers.
3. Method of Claim 1 or 2, wherein the identification number is deleted at the end of a stipulated period of time.
4. Method of one of the preceding Claims, wherein the patient's name and address filed on a Web server and/or database server are saved to an external data medium at the end of a stipulated period of time and deleted from the Web server and/or database server.

5. Method of one of the preceding Claims, wherein the data is encrypted prior to sending and decrypted upon receipt.
6. Method of one of the preceding Claims, wherein the answer is displayed in an invisible frameset.
7. Device for securing patient data in the case of an exchange of information between a patient and a specialist by means of a data network, in particular for performing the method of one of Claims 1 to 6,
wherein
a first Web server and a database server connected to the first Web server are provided, through which the patient's name and address are entered and saved, and through which the patient is assigned an identification number,
a second Web server is provided, through which the patient is able to exchange data with a specialist under his identification number,
the second Web server is connected to the database server, and the first Web server and the second Web server are isolated from each other.
8. Device of Claim 7, wherein physical separation is provided between the first Web server and the database server on the one hand, and between the second Web server and the database server on the other hand.
9. Device of Claim 7 or 8, wherein a second database server is provided, which is connected to the first and/or the second Web server.

10. Device of Claim 7, wherein a backup unit is provided, which saves the data from the database server to an external data medium at regular intervals of time and deletes the data from the database server.
11. Device of Claim 7, wherein a crypto module is provided for the purpose of encrypting and decrypting the data.